29.01.99.C1 Management of Information Resources

Revised: September 17, 2026
Next Scheduled Review: September 17, 2031
Revision History

Rule Summary

This rule is required by The Texas A&M University System (System) Policy *29.01, Information Resources* and outlines the responsibilities of the President, Associate Vice President for Information Technology and Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Digital Accessibility Officer (DAO) related to governing the use of information resources at Texas A&M University-Corpus Christi (TAMU-CC).

Rule

1. GENERAL

    1.1. At TAMU-CC, the CIO fulfills the Information Resource Manager role and the associated responsibilities under Texas Administrative Code (TAC) Chapter 211 unless otherwise delegated by the President.

    1.2. Under the direction of the TAMU-CC President, the CIO is responsible for establishing a University Technology Council (UTC) to review technology initiatives and makes recommendations to the President's Cabinet regarding campus impact, dependencies, risks, adoption, and roadblocks of the initiatives. The President's Cabinet remains the authority for approval, prioritization, and funding of the initiatives. The UTC will also assist in the review of Information Technology (IT) standards as outlined in section 2.3 of this rule.

2. INFORMATION SECURITY

    2.1. In accordance with System Regulation *29.02.01, Information Security Governance,* the President designates the CISO, under the supervision of the CIO and in consultation with the System Chief Information Security Officer (SCISO), to administer the information security requirements of TAC 202 and all applicable laws, policies, and regulations regarding information resources and security.

2.2. Effective security programs will be implemented to mitigate risks posed by existing and/or potential threats to TAMU-CC electronic information resources. Measures will be taken to protect these resources against unauthorized access disclosure, modification or destruction, whether accidental or deliberate.

2.3. The CISO may issue binding and enforceable IT policy in the form of documented IT standards (e.g., IT Acceptable Use, Cybersecurity Controls Catalog). IT standards must not be used to document the broad rights and responsibilities of all users, which must be documented in university rules and procedures. The CISO presents proposed IT standards and proposed changes to or deletions of existing IT standards to the CIO and the IT senior staff for feedback. After review and incorporation of any appropriate feedback the CISO sends the proposal to the UTC, the Vice President for Finance & Administration, and all IT staff, who have 10 business days to respond. The CISO provides any proposed edits submitted during the 10-day response period are provided to the CIO and IT senior staff for additional feedback. The CISO will review all proposed edits and feedback over 10 business days and accept or reject for incorporation in the proposal. Upon approval the proposal becomes official and is posted on a website accessible to all TAMU-CC users. The CISO reviews all IT standards at least annually.

3. ACCESSIBILITY OF DIGITAL INFORMATION RESOURCES

3.1. All faculty and staff must comply with American Disabilities Act (ADA) Title II, TAC 206 and TAC 213, this rule, and related guidelines in the development, procurement, maintenance, or use of digital information resources.

3.2. The President designates the DAO to ensure compliance with this rule. In the absence of a DAO, the CIO will serve as the DAO.

3.3. All websites, web pages, online courses, and web applications owned, funded, developed, procured, maintained, or operated by TAMU-CC whether public-facing or internal must comply with TAC 206 and ADA Title II.

3.4. Compliance Plan

3.4.1. The DAO and CIO are responsible for developing and implementing a Digital Accessibility Plan under which all new and existing digital resources must comply with TAC 206 and TAC 213, as applicable.

3.4.2. The Digital Accessibility Plan will guide compliance with this rule and detail digital accessibility training, monitoring, and procurement guidelines.

3.4.3. The DAO will oversee and provide training in compliance with TAC 206 and TAC 213, this rule, and the Digital Accessibility Plan.

3.5. Exceptions

3.5.1. Any request for an exception under TAC 213 must be submitted to the DAO for review and processing.

3.5.2. The DAO will review requests for exceptions under TAC 213, ensure that requests meet the requirements for an exception, and forward requests to the CIO with a recommendation regarding approval.

3.5.3. The CIO will further review each exception request and forward the request to the President or designee with a recommendation regarding approval.

3.5.4. The DAO will maintain exception requests in accordance with the Texas A&M University System Records Retention Schedule (see Appendix).

3.6. Monitoring

3.6.1. The DAO will monitor purchasing contracts, purchase orders, and procurement card purchases for compliance with 213, this rule, and procurement practices related to digital resources.

3.6.2. The DAO will oversee and monitor the development and maintenance of digital resources and compliance with this rule and TAMU-CC-wide compliance with TAC 206, TAC 213, and ADA Title II where applicable.

3.7. The CIO will provide the necessary technical and review process support to the DAO in fulfilling their responsibilities under this rule.

Related Statutes, Policies, or Requirements

Title II of the Americans with Disabilities Act of 1990 (ADA)
Texas Administrative Code, Chapter 202
Texas Administrative Code, Chapter 206
Texas Administrative Code, Chapter 211
Texas Administrative Code, Chapter 213
System Policy *29.01, Information Resources*
System Regulation *29.01.04, Accessibility of Digital Information Resources*
System Policy *29.02, Information Security*
University Procedure *61.99.99.C0.02, Web Presence*

University IT Standard IT Acceptable Use
University IT Standard Cybersecurity Control Catalog

This rule supersedes:

- *29.01.99.C1, Security of Electronic Information Resources*

Appendix

Texas A&M University System Records Retention Schedule

Contact Office

Contact for interpretation and clarification:	Associate Vice President for Information Technology and Chief Information Officer 361.825.2494